Text References:

[1] Carl F. Endorf, Eugene Schultz, Jim Mellander**,** *Intrusion Detection & Prevention*: The Authoritative Guide to Detecting Malicious Activity

[2] Rafeeq Ur Rehman, *Intrusion Detection Systems with Snort Advanced IDS Techniques* Using Snort, Apache, MySQL, PHP, and ACID

[3] Rebecca Bace, "*Intrusion Detection*", Macmillan Technical Publishing, 2000.

[4] Rebecca Bace and Peter Mell, "*Intrusion Detection Systems*" http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf, 2001

[5] Rubecca gurley**,** *Intrusion detection*

[6] Stephen Northcutt and Judy Novak**,** *Network Intrusion Detection*

Webliography:

[01] A. Jones and R. Sielken, “Computer intrusion detection: A survey,” University of Virginia, Computer Science, Tech. Rep., 2000.

[02] A. Somayaji and S. Forrest, “Automated response using system-call delays,” in Proceedings of Usenix Security Symposium, 2000, pp. 185–198.

[03] “Agilent 66300 series data sheet,” Agilent. Available: http://www.home.agilent.com /upload/cmcupload/All/66300series datasheet May04.pdf

[04] Centrax page, http://www.cybersafe.com

[05] Diego Zamboni, "Using Internal Sensors for Computer Intrusion Detection", PHD thesis, <http://www.cerias.purdue.edu/techreports-ssl/ public/2001-42.pdf>, 2001

[06] E. Lundin and E. Jonsson, “Survey of intrusion detection research,” Chalmers University, Tech. Rep., February 2002.

[07] F. Stajano and R. Anderson, “The resurrecting duckling: Security issues for adhoc wireless networks,” in Proceedings of the 7th International Workshop on Security Protocols, Lecture Notes in Computer Science volume 1796, April 1999, pp. 172–194.

[08]“Freshdiagnose,”FreshDevices.Available:http://www.freshdevices.com/freshdiag.html

[09] Hervé Debar, “A Revised Taxonomy for Intrusion Detection”, IBM Research, <http://www.security technet.com/resources/rsccenter/vendorwp/ibm/ibms urvey.ps>, 1999

[10]http://www.sans.org/reading_room/whitepapers/detection/protocol_anomaly_detection_for_ networkbased_intrusion_detection_349?show=349.php&cat=detection

[11] “Iperf bandwidth measurement tool,” NLANR Distributed Application Support Team.[Online]. Available: http://dast.nlanr.net/Projects/Iperf/

[12] “I8kfangui,” Christian Diefer. Available: http://www.diefer.de/i8kfan/

[13] J. Balthrop and S. a. Forrest, “Revisiting lisys: Parameters and normal behavior,” in Proceedings of the Congress on Evolutionary Computing, 2002.

[14] J.M. Bradshaw, "An introduction to software agents", AAA1 Press/MIT Press, Cambridge, 1997

[15] J. Krishnaswami, “Denial-of-service attacks on battery-powered mobile computers,”Master’s thesis, Virginia Tech, 2004.

[16] J. Milton and J. C. Arnold, Introduction to Probability and Statistics, 3rd ed. Irwin McGraw-Hill, 1995, pp. 382–491.

[17] Martin Arvidson and Markus Carlbark, "Intrusion Detection Systems - Technologies, Weaknesses andTrends",<http://www.ep.liu.se/exjobb/isy/2003/330/ exjobb.pdf>, 2003.

[18] Mikhail Gordeev, "Intrusion Detection: Techniques and Approaches", http://www.cosc.canterbury.ac.nz/research/ RG/i-net_security/IDSIEEE.pdf>, 2000

[19] "Microsoft performance data counters," Microsoft. Available: http://msdn.microsoft.com/ library/default.asp?url=/library/en-us/perfmon/ base/performance data.asp

[20] M. Satyanarayanan, "Pervasive computing: vision and challenges," IEEE Personal Communications, vol. 8, no. 4, pp. 10–17, August 2001.

[21] Naval Information Systems Management Center, US, "Introduction to Information Systems Security Guidebook",<http://www.marcorsyscom.usmc.mil/ sites/ia/references/intro.pdf>, 1995

[22] Ofir Arkin, "Network Scanning Techniques Understanding how it is done", <http://downloads. securityfocus.com/library/Network_Scanning_Techniques.pdf>, 1999

[23] "Openssh for windows," Michael Johnson. Available: http://sshwindows.sourceforge.net/

[24] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptography, pp. 388–397, 1999.

[25] RealSecure page,<http://www.iss.net/prod/rs.html

[26] Rijndael page, <http://www.esat. kuleuven.ac.be/~rijmen/rijndael/>.

[27] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Chalmers University, Tech. Rep. 99-15, March 2000.

[28] "Symbos.cabir," Corporation, Symantec.Available:http://securityresponse.symantec.com/ avcenter/venc/data/epoc.cabir.html

[29] T. Martin, M. Hsiao, D. S. Ha, and J. Krishnaswami, "Denial-of-service attacks on batter-powered mobile computers," in Second IEEE International Conference on Pervasic Computing and Communications, vol. 8, no. 4, March 2004.

[30] T. M. Mudge, "Power: A first-class architectural design constraint," IEEE Computer, vol. 34, no. 4, pp. 52–58, 2001.

[31] "The intel pentium m processor: Microarchitecture and performance," Intel.[Online]. Available: http://www.intel.com/technology/itj/2003/volume07issue02/art03 pentiumm/p10 speedstep.htm

[32] W. Lee and S. Stolfo, “Data mining approaches to intrusion detection,” in Proceedings of the 7th USENIX Security Symposium, January 1998, pp. 77–94.